DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

System Name Check (SYNCH)

PIA Completion Date: FY 2008, Quarter 3

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)
Email: pia@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

Does this system collect, maintain or disseminate *personally identifiable information* about individual members of the public?**

Personally identifiable information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

Individual members of the public means **any person not acting in his/her official capacity as a federal government employee/contractor**. This definition may include but is not limited to:

- U.S. citizens whether natural born or naturalized;
- Legal Permanent Resident Aliens (LPRs);
- Aliens;
- Federal government employee/contractor acting solely in his/her own personal capacity.

YES X NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail address: pia@state.gov.

[System of Records - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned]

1) Does a Privacy Act system of records already exist?

YES __X__ NO

If yes, please provide the following:
System Name: Diplomatic Security Records Number STATE-36

If no, a Privacy system of records description will need to be created for this data.

2) What is the purpose of the system/application?

The SYNCH application falls under the auspices of the Bureau of Diplomatic Security (DS), Office of Personnel Security & Suitability (DS/SI/PSS), which is the headquarters element in charge of all domestic tasks, associated with tracking personnel clearance status and Clearance Folder Locations for DS.

SYNCH lends itself to capturing and maintaining data specific to: (1) administrative and operational case control of all new hires and certain contractors, as it relates to personnel clearances; (2) periodic re-investigation on current DS employees and contractors, which depending upon the level of clearance over a five year time-span; (3) adjudication of sensitive reports of investigation involving misconduct, criminal behavior, or counter intelligence matters concerning DS employees and contractor; whereby the adjudication often results in the suspension an subsequent revocation of access and may involve an appeal process;, and (4) maintenance of DS Historical Data/Information specific to Security Clearance Determinations, based on the best interests of National Security.

The **Case File** contains all pertinent applicant information, to include name, social security number, b ate of Birth, addresses (past and current), employer (past and current), and all critical information associated with the Case File.

3) What legal authority authorizes the purchase or development of this system/application?

The legal authorities as documented in STATE-36, Diplomatic Security Records.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

The categories of individuals who are covered by the system are documented in STATE-36, Diplomatic Security Records.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

The source of the information is the individual or law enforcement agencies.

b. What type of information is collected from the source of the information?

The source provides all personally identifiable information (PII) that is then maintained in the **case file.** This information includes, name, social security number, date of birth, address (past and current), employer (past and current), and all other critical information that supports the case file.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The agency or source providing the information is responsible for verifying accuracy.

b. How will data be checked for completeness?

Completeness of data will be checked through investigations and/or through personal interviews of the information source.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Investigations and/or personal interviews will confirm whether data is current.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes, SYNCH lends itself to capturing and maintaining data specific to: (1) administrative and operational case control of all new hires and certain contractors, as it relates to personnel clearances; (2) periodic re-investigation on current DS employees and contractors, which depending upon the level of

clearance over a five year time-span; (3) adjudication of sensitive reports of investigation involving misconduct, criminal behavior, or counter intelligence matters concerning DoS employees and contractor; whereby the adjudication often results in the suspension an subsequent revocation of access and may involve an appeal process; and (4) maintenance of DS Historical Data/Information specific to Security Clearance Determinations, based on the best interests of National Security.

2) **Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

No.

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

No.

4) **Will the new data be placed in the individual's record?**

Yes, the information will be placed in either the existing investigative file or in an existing background security file.

5) **How will the new data be verified for relevance and accuracy?**

Verification will be made through investigations and/or personal interviews.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

The data will be retrieved by PII (e.g., name, social security number, and any other PII that is available).

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

No reports will be produced on individuals.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The system is operated only at one site, State Annex-20 (SA-20).

2) What are the retention periods of data in this system?

The retention period of data is consistent with established Department of State Policies and Guidelines as documented in the Department's Disposition Schedule for Diplomatic Security Records, Chapter 11.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The retention period of data is consistent with established Department of State Policies and Guidelines, as documented in the Department's Disposition Schedule for Diplomatic Security Records, Chapter 11.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy and does it restrict access to the system?

No additional or new effect to privacy. Yes, access restrictions are in place.

6) If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?

N/A

7) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

8) Are there forms associated with the system? YES ___ NO X

If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA:

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

   Access to the data in the system is on "a need to know" basis and/or under routine use criteria as explained in STATE-36.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

   Criteria for gaining access to the system are on "a need-to-know basis." Criteria, procedures, controls and responsibilities regarding access are all documented.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   Access will be restricted on "a need to know" basis—specific to work related responsibilities.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**

   The system provides a means of limiting access to areas within the application based on user ID, password, and "a need to know." Moreover, Bureau of Diplomatic Security, Domestic Operations, Office of Personnel Security & Suitability (DS/SI/PSS) employees and contractor must follow the System Behavior Rules established by the Department.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? YES

   If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? YES

Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended? YES

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   No.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, and Other)? If so, how will the data be used by the other agency?**

   Other agencies will not have direct access to the data but the data may be shared with an agency upon request from that agency if that agency is listed as a routine user in STATE-36. The use of the data by the other agency will be restricted to the same purpose for which the data was originally collected.

8) **Who is responsible for assuring proper use of the SHARED data?**

   The agency receiving the information is responsible for adhering to lawful restrictions.